มาตรฐานอาชีพและคุณวุฒิวิชาชีพ
Occupational Standard and Professional Qualifications

สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาธุรกิจดิจิทัลและพาณิชย์อิเล็กทรอนิกส์

จัดทำโดย สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน)

1. ชื่อมาตรฐานอาชีพ

สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาธุรกิจดิจิทัลและพาณิชย์อิเล็กทรอนิกส์

2. ประวัติการปรับปรุงมาตรฐาน

N/A

3. ทะเบียนอ้างอิง (Imprint)

N/A

4. ข้อมูลเบื้องต้น

ปัจจุบันธุรกิจมีการนำเทคโนโลยีสารสนเทศเข้ามาเป็นเครื่องมือในการทำธุรกิจ ทำให้มีความสามารถทางพาณิชย์กรรมในรูปแบบอิเล็กทรอนิกส์ เรียกว่า พาณิชย์อิเล็กทรอนิกส์ โดยประโยชน์ที่ธุรกิจได้รับจากการทำพาณิชย์อิเล็กทรอนิกส์มีหลายประการ ได้แก่ การเข้าถึงลูกค้าโดยไร้ข้อจำกัดด้านสถานที่และเวลา การนำเสนอรายละเอียดสินค้าได้หลากหลายมากขึ้น ลูกค้าสามารถค้นหาสินค้าได้ตรงกับความต้องการ การรับคำสั่งซื้อ การลดค่าใช้จ่าย รวมถึงการนำข้อมูลมาวิเคราะห์ทางการตลาด ช่วยส่งเสริมให้ธุรกิจมีความสามารถในการค้าขายมากขึ้น ซึ่งธุรกิจที่มีศักยภาพด้านพาณิชย์อิเล็กทรอนิกส์ช่วยส่งผลต่อความสามารถในการแข่งขันระดับประเทศ

หน่วยงานภาครัฐ เป็นหน่วยงานที่ช่วยสนับสนุนให้การทำพาณิชย์อิเล็กทรอนิกส์ ให้ดำเนินไปได้อย่างสะดวกรวดเร็ว มีความน่าเชื่อถือ และมีความปลอดภัย เนื่องจากวิธีการทำพาณิชย์อิเล็กทรอนิกส์เป็นรูปแบบที่เปลี่ยนแปลงไปจากเดิมที่เคยปฏิบัติ มีเครื่องมือและวิธีการใหม่ ๆ ที่ธุรกิจและบุคลากรที่เกี่ยวข้องต้องเข้าใจในสิ่งแปลงใหม่เหล่านี้ ถึงแม้ว่าปัจจุบันธุรกิจได้มีการทำธุรกรรมในรูปแบบพาณิชย์อิเล็กทรอนิกส์มาสักระยะแล้วก็ตาม แต่การจัดหาบุคลากรที่มีความรู้ตรงกับความต้องการยังมีความจำเป็น จึงควรมีการประเมินความรู้ของแรงงานที่มีความรู้และทักษาได้ตรงกับลักษณะงาน จึงควรมีการกำหนดให้มีการประเมินสมรรถนะความรู้และทักษะในการปฏิบัติงานดังกล่าว

การวัดสมรรถนะเป็นการประเมินคุณลักษณะในด้าน ทักษะ ความรู้ ความสามารถ สำหรับอาชีพนักพาณิชย์อิเล็กทรอนิกส์ เป็นการบูรณาการความรู้ ได้แก่ ด้านเทคโนโลยีสารสนเทศ ซึ่งประกอบไปด้วยโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและความรู้ในการออกแบบและพัฒนาเว็บเพื่อค้าขาย ด้านการตลาดซึ่งประกอบด้วยกลยุทธ์การตลาดและการให้คำปรึกษาแก่ธุรกิจ โดยความรู้ที่กล่าวมานี้ ผู้ปฏิบัติงานจำเป็นต้องมีสมรรถนะในการปฏิบัติงาน ซึ่งมีความแตกต่างกันไป ตามลักษณะงานของพาณิชย์อิเล็กทรอนิกส์ที่รับผิดชอบ

5. ประวัติการปรับปรุงมาตรฐานในแต่ละครั้ง

N/A

6. ครั้งที่

ครั้งที่ 1/2566

7. คุณวุฒิวิชาชีพที่ครอบคลุม (Professional Qualifications included)

สาขาวิชาชีพอุตสาหกรรมดิจิทัล

สาขาธุรกิจดิจิทัลและพาณิชย์อิเล็กทรอนิกส์

นักบริหารระบบความมั่นคงปลอดภัยด้านพาณิชย์อิเล็กทรอนิกส์ ระดับ 6

8. คุณวุฒิวิชาชีพที่เกี่ยวข้อง (Related Professional Qualifications)

N/A

9. หน่วยสมรรถนะทั้งหมดในมาตรฐานอาชีพ (List of All Units of Competence within this Occupational Standards)

รหัสหน่วยสมรรถนะ	**เนื้อหา**
1025	ปฏิบัติตามจรรยาบรรณ กฎหมายและความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์
2021	บริหารจัดการระบบความมั่นคงปลอดภัยด้านเว็บไซต์

10. ระดับคุณวุฒิ

10.1 สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาธุรกิจดิจิทัลและพาณิชย์อิเล็กทรอนิกส์ นักบริหารระบบความมั่นคงปลอดภัยด้านพาณิชย์อิเล็กทรอนิกส์ ระดับ 6

คุณลักษณะของผลการเรียนรู้ (Characteristics of Outcomes)

เป็นผู้ที่มีสมรรถนะด้านผู้บริหารจัดการระบบความมั่นคงด้านอีคอมเมิร์ซ โดยจะต้องมีความรู้
ความสามารถเกี่ยวกับการบริหารจัดการระบบความมั่นคงปลอดภัยด้านเว็บไซต์อย่างมีประสิทธิภาพ
การบริหารจัดการบริการโครงสร้างพื้นฐานด้านอีคอมเมิร์ซอย่างมีความมั่นคงปลอดภัยตามข้อกำหนดที่เกี่ยวข้อง
และการบริหารจัดการระบบความมั่นคงปลอดภัยขั้นพื้นฐานด้านอีคอมเมิร์ซอย่างมีประสิทธิภาพ โดยเป็นบุคคลที่มีคุณลักษณะของผลการเรียนรู้ ดังนี้

1. มีความรู้พื้นฐานการคำนวณ และการวิเคราะห์ข้อมูลเบื้องต้น
2. มีทักษะการสื่อสาร ประสานงานด้วยภาษาไทย ภาษาต่างประเทศหรือภาษาในประเทศอาเซียน
3. มีส่วนร่วมในการวางแผน และพัฒนากระบวนการทำงาน
4. สามารถใช้องค์ความรู้หรือนวัตกรรม เพื่อแก้ปัญหาที่ซับซ้อนมีการเปลี่ยนแปลงตลอดเวลา ด้วยการคิดเชิงกลยุทธ์และใช้ศาสตร์ที่หลากหลาย
5. มีความรู้การบริหารจัดการกลยุทธ์และใช้องค์ความรู้หรือนวัตกรรม เพื่อแก้ปัญหางานที่ซับซ้อนมีการเปลี่ยนแปลงตลอดเวลา
6. สามารถประยุกต์ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงาน
7. เรียนรู้และการประเมินผลการทำงานของตนเองได้
8. มีคุณธรรมและจริยธรรม

การเลื่อนระดับคุณวุฒิวิชาชีพ (Qualification Pathways)

1. ผู้ขอเข้ารับการประเมินคุณวุฒิวิชาชีพ นักบริหารระบบความมั่นคงปลอดภัยด้านพาณิชย์อิเล็กทรอนิกส์ ระดับ 6
ต้องเป็นผู้ที่มีประสบการณ์ทำงานด้านการบริหารจัดการระบบความมั่นคงปลอดภัยเกี่ยวกับพาณิชย์อิเล็กทรอนิกส์ อย่างน้อย 1 ปี โดยมีเอกสารหลักฐานรับรอง
2. การได้รับการรับรองคุณวุฒิวิชาชีพสาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาธุรกิจดิจิทัลและพาณิชย์อิเล็กทรอนิกส์
นักบริหารระบบความมั่นคงปลอดภัยด้านพาณิชย์อิเล็กทรอนิกส์ ระดับ 6 ผู้ขอเข้ารับการประเมินต้องผ่านเกณฑ์การประเมินตามหน่วยสมรรถนะในคุณวุฒิวิชาชีพนี้
จำนวนทั้งหมด 2 หน่วยสมรรถนะ

หลักเกณฑ์การต่ออายุหนังสือรับรองมาตรฐานอาชีพ

N/A

กลุ่มบุคคลในอาชีพ (Target Group)

บุคคลในกลุ่มอาชีพนักบริหารระบบความมั่นคงปลอดภัยด้านพาณิชย์อิเล็กทรอนิกส์ เช่น ผู้บริหารความมั่นคงเว็บ ผู้บริหารความมั่นคงเครือข่าย ผู้บริหารเว็บโฮสต์ เป็นต้น

หน่วยสมรรถนะ (หน่วยสมรรถนะทั้งหมดของคุณวุฒิวิชาชีพนี้)

1025 ปฏิบัติตามจรรยาบรรณ กฎหมายและความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์
2021 บริหารจัดการระบบความมั่นคงปลอดภัยด้านเว็บไซต์

ตารางแผนผังแสดงหน้าที่

1. ตารางแสดงหน้าที่ 1

ประกาศใช้ ณ 19/05/2565

ตาราง 1 : FUNCTIONAL MAP แสดง KEY PURPOSE , KEY ROLES , KEY FUNCTION

ความมุ่งหมายหลัก Key Purpose	บทบาทหลัก Key Roles		หน้าที่หลัก Key Function	
คำอธิบาย	รหัส	คำอธิบาย	รหัส	คำอธิบาย
ให้บริการด้านพาณิชย์อิเล็กทรอนิกส์และเว็บไซต์อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัยในระดับสากล	20	บริหารจัดการเว็บไซต์ (Web Hosting)	202	บริหารระบบความมั่นคงปลอดภัยด้านพาณิชย์อิเล็กทรอนิกส์
	10	ให้คำปรึกษาและบริหารด้านพาณิชย์อิเล็กทรอนิกส์และด้านการตลาดดิจิทัล	102	บริหารจัดการด้านพาณิชย์อิเล็กทรอนิกส์และด้านการตลาดดิจิทัล

คำอธิบาย ตารางแผนผังแสดงหน้าที่เป็นแผนผังที่ใช้วิเคราะห์หน้าที่งานเพื่อให้ได้หน้าที่หลัก (Key Function)

2. ตารางแสดงหน้าที่ 1 (ต่อ)

ประกาศใช้ ณ 19/05/2565

ตาราง 2 : FUNCTIONAL MAP แสดง KEY FUNCTION , UNIT OF COMPETENCE , ELEMENT OF COMPETENCE

หน้าที่หลัก Key Function		หน่วยสมรรถนะ Unit of Competence		หน่วยสมรรถนะย่อย Element of Competence	
รหัส	**คำอธิบาย**	**รหัส**	**คำอธิบาย**	**รหัส**	**คำอธิบาย**
102	บริหารจัดการด้านพาณิชย์อิเล็กทรอนิกส์และด้านการตลาดดิจิทัล	1025	ปฏิบัติตามจรรยาบรรณ กฎหมายและความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์	10251	ปฏิบัติตามจรรยาบรรณวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์
				10252	ปฏิบัติตามกฎหมายพาณิชย์อิเล็กทรอนิกส์
				10253	ปฏิบัติความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์
202	บริหารระบบความมั่นคงปลอดภัยด้านพาณิชย์อิเล็กทรอนิกส์	2021	บริหารจัดการระบบความมั่นคงปลอดภัยด้านเว็บไซต์	20211	วางแผนเพื่อบริหารจัดการความมั่นคงปลอดภัยเว็บไซต์
				20212	ตั้งค่าความมั่นคงปลอดภัยเครื่องบริการเว็บได้
				20213	ใช้โปรแกรมประยุกต์ความมั่นคงปลอดภัยบนเครื่องบริการเว็บเพื่อให้บริการ
				20214	รับมือสถานการณ์ภัยคุกคามที่เกิดกับเว็บไซต์

คำอธิบาย

ตารางแผนผังแสดงหน้าที่ (ต่อ) เป็นแผนผังที่ใช้วิเคราะห์หน้าที่งานหลังจากได้หน้าที่หลัก (Key Function) เพื่อให้ได้ หน่วยสมรรถนะ (Unit of Competence) และหน่วยสมรรถนะย่อย (Element of Competence)

1. รหัสหน่วยสมรรถนะ 1025

2. ชื่อหน่วยสมรรถนะ ปฏิบัติตามจรรยาบรรณ กฎหมายและความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์

3. ทบทวนครั้งที่ 1 / 2566

4. สร้างใหม่ ☐ **ปรับปรุง** ☑

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

1.ที่ปรึกษาด้านพาณิชย์อิเล็กทรอนิกส์
2.นักพาณิชย์อิเล็กทรอนิกส์
3.นักการตลาดดิจิทัล
4.นักบริหารจัดการระบบบริการออนไลน์
5.นักบริหารระบบความมั่นคงปลอดภัยด้านพาณิชย์อิเล็กทรอนิกส์
6.นักประเมินระบบพาณิชย์อิเล็กทรอนิกส์
7.นักพัฒนาระบบเว็บไซต์ด้านพาณิชย์อิเล็กทรอนิกส์
8.นักออกแบบเว็บไซต์

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

บุคคลที่ทำหน้าที่เกี่ยวกับการปฏิบัติตามจรรยาบรรณวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์ ปฏิบัติตามกฎหมายพาณิชย์อิเล็กทรอนิกส์ และปฏิบัติความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☐	☑	☐	☐

8. กลุ่มอาชีพ (Sector)

กลุ่มวิชาชีพอุตสาหกรรมดิจิทัล สาขาธุรกิจดิจิทัลและพาณิชย์อิเล็กทรอนิกส์

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

N/A

10. ข้อกำหนดหรือกฎระเบียบที่เกี่ยวข้อง (Licensing or Regulation Related) (ถ้ามี)

กฎหมายที่เกี่ยวข้องกับ กฎหมายพาณิชย์อิเล็กทรอนิกส์ ได้แก่ กฎหมายธุรกรรมพาณิชย์อิเล็กทรอนิกส์ กฎหมายคุ้มครองข้อมูล กฎหมายอาชญากรรมทางคอมพิวเตอร์ กฎหมายการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ กฎหมายลายมือชื่อทางอิเล็กทรอนิกส์ กฎหมายการโอนเงินทางอิเล็กทรอนิกส์ กฎหมายโทรคมนาคม กฎหมายที่เกี่ยวเนื่องกับอินเตอร์เน็ต กฎหมายพัฒนาเทคโนโลยีและอุตสาหกรรมอิเล็กทรอนิกส์และคอมพิวเตอร์ กฎหมายทรัพย์สินทางปัญญา

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
10251 ปฏิบัติตามจรรยาบรรณวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์	1.มีจริยธรรมในการประกอบวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์ 2.ใช้ทรัพยากรและข้อมูลอย่างสุจริต 3.รักษาความลับข้อมูลส่วนบุคคลและข้อมูลสำคัญองค์การ 4.ปฏิบัติงานโดยใช้หลักจรรยาบรรณวิชาชีพ	ข้อสอบข้อเขียน การสัมภาษณ์ แฟ้มสะสมผลงาน
10252 ปฏิบัติตามกฎหมายพาณิชย์อิเล็กทรอนิกส์	1.เลือกใช้กฎหมายเพื่อนำมาใช้ในการปฏิบัติงานในหน่วยงาน 2.ดำเนินงานตามข้อกำหนดและข้อบังคับใช้กฎหมาย 3.ระบุบทลงโทษที่เกี่ยวข้องกับการปฏิบัติงานด้านพาณิชย์อิเล็กทรอนิกส์	ข้อสอบข้อเขียน การสัมภาษณ์ แฟ้มสะสมผลงาน
10253 ปฏิบัติความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์	1.ป้องกันภัยคุกคามด้านความมั่นคงปลอดภัย 2.ปฏิบัติตามหลักการเพื่อรักษาความปลอดภัย	ข้อสอบข้อเขียน การสัมภาษณ์ แฟ้มสะสมผลงาน

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

N/A

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. ปฏิบัติตามจรรยาบรรณวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์
2. ปฏิบัติตามกฎหมายพาณิชย์อิเล็กทรอนิกส์
3. ปฏิบัติความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์

(ข) ความต้องการด้านความรู้

1. จรรยาบรรณ และจริยธรรมในวิชาชีพ
2. กฎหมายพาณิชย์อิเล็กทรอนิกส์
3. ความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์
4. การใช้ระบบเทคโนโลยีสารสนเทศและการติดต่อสื่อสาร
5. การพาณิชย์อิเล็กทรอนิกส์

14. หลักฐานที่ต้องการ (Evidence Guide)

หลักฐานที่ต้องการจะกำหนดข้อแนะนำเกี่ยวกับการประเมิน และควรที่จะใช้ประกอบร่วมกันกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. เอกสารการประเมินการสัมภาษณ์
2. แฟ้มสะสมผลงาน

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. เอกสารผ่านการอบรมเกี่ยวกับการปฏิบัติตามจรรยาบรรณ กฎหมายและความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์
2. เอกสารรับรองการผ่านการสอบข้อเขียนหรือผลการทดสอบความรู้(ค) คำแนะนำในการประเมิน

ประเมินเกี่ยวกับการปฏิบัติตามจรรยาบรรณ กฎหมายและความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์ โดยพิจารณาจากหลักฐานที่เกี่ยวข้องทั้งหลักฐานการปฏิบัติงานและหลักฐานด้านความรู้

(ง) วิธีการประเมิน

1. พิจารณาหลักฐานความรู้
2. พิจารณาหลักฐานการปฏิบัติงาน

15. ขอบเขต (Range Statement)

ขอบเขตอธิบายถึงขอบเขตของการปฏิบัติงาน และสภาพแวดล้อมอื่น ๆ หรือสถานการณ์อื่น ๆ ที่มีผลกระทบต่อการทำงาน รวมถึงเครื่องมือ อุปกรณ์ เทคโนโลยี ทรัพยากรที่ใช้ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

(ก) คำแนะนำ

การปฏิบัติตามจรรยาบรรณ กฎหมายและความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์ ผู้เข้ารับการประเมินจะต้องแสดงเกี่ยวกับการมีจริยธรรมในการประกอบวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์ การใช้ทรัพยากรและข้อมูลอย่างสุจริต การรักษาความลับข้อมูลส่วนบุคคลและองค์การ และการปฏิบัติงานโดยใช้หลักจรรยาบรรณวิชาชีพ การเลือกใช้กฎหมายเพื่อนำมาใช้ในการปฏิบัติงานในหน่วยงาน การดำเนินงานตามข้อกำหนดและข้อบังคับใช้กฎหมาย และการระบุบทลงโทษที่เกี่ยวข้องกับการปฏิบัติงานด้านพาณิชย์อิเล็กทรอนิกส์ รวมถึงการป้องกันภัยคุกคามด้านความมั่นคงปลอดภัย และการปฏิบัติตามหลักการเพื่อรักษาความปลอดภัย

(ข) คำอธิบายรายละเอียด

1. จรรยาบรรณ และจริยธรรมในวิชาชีพ

จรรยาบรรณการใช้เทคโนโลยีสารสนเทศหมายถึง หลักศีลธรรมจรรยาที่กำหนดขึ้นเพื่อใช้เป็น แนวทางปฏิบัติ หรือควบคุมการใช้ระบบคอมพิวเตอร์และสารสนเทศความสำคัญ คือ จรรยาบรรณการใช้เทคโนโลยีสารสนเทศทำให้การใช้อินเทอร์เน็ตเป็นไปอย่างสงบสุข ไม่เกิดปัญหาการละเมิดลิขสิทธิ์ อาชญากรรม การขโมยผลงานของคนอื่น การมีความเป็นส่วนตัวและการใช้งานอินเทอร์เน็ตไม่สร้างความรำคาญหรือรบกวนคนอื่น เป็นต้น ทำให้สังคมเป็นสุข

จรรยาบรรณนักคอมพิวเตอร์

1.มีความซื่อสัตย์ต่อตนเองและผู้อื่น
2.ไม่ละทิ้งงานในหน้าที่ ที่ได้รับมอบหมาย
3.ไม่เปิดเผยข้อมูลที่เป็นความลับกับผู้อื่น
4.มีความจงรักภักดีต่อองค์กร
5.อุทิศตนให้กับวิชาชีพอย่างเต็มกำลังความสามารถ
6.ไม่ทุจริตและคอรัปชั่น
7.มีความรักและศรัทธาต่ออาชีพ
จรรยาบรรณสำหรับผู้ใช้อินเทอร์เน็ต
1.ต้องไม่ใช้คอมพิวเตอร์ทำร้าย หรือละเมิดผู้อื่น
2.ต้องไม่รบกวนการทำงานของผู้อื่น
3.ต้องไม่สอดแนม แก้ไข หรือเปิดดูแฟ้มข้อมูลของผู้อื่น
4.ต้องไม่ใช้คอมพิวเตอร์เพื่อการโจรกรรมข้อมูลข่าวสาร
5.ต้องไม่ใช้คอมพิวเตอร์สร้างหลักฐานที่เป็นเท็จ
6.ต้องไม่คัดลอกโปรแกรมของผู้อื่นที่มีลิขสิทธิ์
7.ต้องไม่ละเมิดการใช้ทรัพยากรคอมพิวเตอร์โดยที่ตนเองไม่มีสิทธิ์
8.ต้องไม่นำเอาผลงานของผู้อื่นมาเป็นของตน
9.ต้องคำนึงถึงสิ่งที่จะเกิดขึ้นกับสังคม อันติดตามมาจากการกระทำของท่าน
10.ต้องใช้คอมพิวเตอร์โดยเคารพกฎระเบียบ กติกา และมีมารยาท
จริยธรรมในการใช้เทคโนโลยีสารสนเทศ

โดยทั่วไปเมื่อพิจารณาถึงคุณธรรมจริยธรรมเกี่ยวกับการใช้เทคโนโลยีคอมพิวเตอร์และ สารสนเทศแล้ว จะกล่าวถึงใน 4 ประเด็น ที่รู้จักกันในลักษณะตัวย่อว่า PAPAประกอบด้วย
ความเป็นส่วนตัว (Information Privacy) หมายถึง สิทธิที่จะอยู่ตามลำพัง และเป็นสิทธิที่เจ้าของสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับ ผู้อื่น สิทธินี้ใช้ได้ครอบคลุมทั้งปัจเจกบุคคล กลุ่มบุคคล และองค์การต่างๆ ปัจจุบันมีประเด็นเกี่ยวกับความเป็นส่วนตัวที่เป็นข้อหน้าสังเกตดังนี้
1.1. การ เข้าไปดูข้อความในจดหมายอิเล็กทรอนิกส์และการบันทึกข้อมูลในเครื่อง คอมพิวเตอร์ รวมทั้งการบันทึก-แลกเปลี่ยนข้อมูลที่บุคคลเข้าไปใช้บริการเว็บไซต์และกลุ่มข่าวสาร
1.2. การ ใช้เทคโนโลยีในการติดตามความเคลื่อนไหวหรือพฤติกรรมของบุคคล ซึ่งทำให้สูญเสียความเป็นส่วนตัว ซึ่งการกระทำเช่นนี้ถือเป็นการผิดจริยธรรม
1.3. การใช้ข้อมูลของลูกค้าจากแหล่งต่างๆ เพื่อผลประโยชน์ในการขยายตลาด1.4.การ รวบรวมหมายเลขโทรศัพท์ ที่อยู่อีเมล์ หมายเลขบัตรเครดิต และข้อมูลส่วนตัวอื่นๆ เพื่อนำไปสร้างฐานข้อมูลประวัติลูกค้าขึ้นมาใหม่ แล้วนำไปขายให้กับบริษัทอื่น ดังนั้น เพื่อเป็นการป้องกันการละเมิดสิทธิความเป็นส่วนตัวของข้อมูลและสารสนเทศ จึงควรจะต้องระวังการให้ข้อมูล โดยเฉพาะการใช้อินเตอร์เน็ตที่มีการใช้โปรโมชั่น หรือระบุให้มีการลงทะเบียนก่อนเข้าใช้บริการ เช่น ข้อมูลบัตรเครดิต และที่อยู่อีเมล์
ความถูกต้อง (Information Accuracy) ในการใช้คอมพิวเตอร์เพื่อการรวบรวม จัดเก็บ และ เรียกใช้ข้อมูลนั้น คุณลักษณะที่สำคัญประการหนึ่ง คือ ความน่าเชื่อถือได้ของข้อมูล ทั้งนี้ จะขึ้นอยู่กับความถูกต้องในการบันทึกข้อมูลด้วย
โดยทั่วไปจะพิจารณาว่าใครจะเป็นผู้รับผิดชอบต่อความถูกต้องของข้อมูลที่จัดเก็บและเผยแพร่ ดังนั้น ในการจัดทำข้อมูลและสารสนเทศให้มีความถูกต้องและ น่าเชื่อถือนั้น ข้อมูลควรได้รับการตรวจสอบความถูกต้องก่อนที่จะนำเข้าฐานข้อมูล รวมถึงการปรับปรุงข้อมูลให้มีความทันสมัยอยู่เสมอ นอกจากนี้ ควรให้สิทธิแก่บุคคลในการเข้าไปตรวจสอบความถูกต้องของข้อมูลตนเองด้วย
ความเป็นเจ้าของ (Information Property) สิทธิความเป็นเจ้าของ หมายถึง กรรมสิทธิ์ในการถือครองทรัพย์สิน ซึ่งอาจเป็นทรัพย์สินทั่วไปที่จับต้องได้ เช่น คอมพิวเตอร์ รถยนต์ หรืออาจเป็นทรัพย์สินทางปัญญา (ความคิด) ที่จับต้องไม่ได้ เช่น บทเพลงโปรแกรมคอมพิวเตอร์ แต่สามารถถ่ายทอดและบันทึกลงในสื่อต่างๆ ได้ เช่น สิ่งพิมพ์ เทปซีดีรอม เป็นต้น โดยในการคัดลอกโปรแกรมคอมพิวเตอร์ให้กับเพื่อน เป็นการกระทำที่จะต้องพิจารณาให้รอบคอบก่อนว่าโปรแกรมที่จะทำการคัดลอกนั้น เป็นโปรแกรมคอมพิวเตอร์ที่ท่านมีสิทธิ์ในระดับใด
การเข้าถึงข้อมูล (Data Accessibility) ปัจจุบันการเข้าใช้งานโปรแกรม หรือระบบ คอมพิวเตอร์มักจะมีการกำหนดสิทธิตามระดับของผู้ใช้งาน ทั้งนี้ เพื่อเป็นการป้องกันการเข้าไปดำเนินการต่างๆ กับข้อมูลของผู้ใช้ที่ไม่มีส่วนเกี่ยวข้อง และเป็นการรักษาความลับของข้อมูล ดังนั้น ในการพัฒนาระบบคอมพิวเตอร์จึงได้มีการออกแบบระบบรักษาความปลอดภัยในการเข้าถึงของผู้ใช้ และการเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับความยินยอมนั้น ก็ถือเป็นการผิดจริยธรรมเช่นเดียวกับการละเมิดข้อมูลส่วนตัว

2. กฎหมายที่เกี่ยวข้องกับพาณิชย์อิเล็กทรอนิกส์
2.1 กฎหมายธุรกรรมพาณิชย์อิเล็กทรอนิกส์
กฎหมายนี้จะต้องสอดคล้องกับกฎหมายระหว่างประเทศ และเหมาะสมกับสภาพของประเทศไทย ทั้งนี้ กฎหมายดังกล่าวรวมถึงกฎหมายธุรกรรมอิเล็กทรอนิกส์ (Electronic

Transaction Law) กฎหมาย ลายเซ็นอิเล็กทรอนิกส์ (Electronic Signature Law) กฎหมาย ธุรกรรมทางการเงินอิเล็กทรอนิกส์ (Electronic Financial Transaction Law) กฎหมายอาญาอันเนื่องมาจากอาชญากรรม พาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce Criminal Code)

2.2 กฎหมายคุ้มครองข้อมูล

เพื่อคุ้มครองสิทธิในความเป็นส่วนตัวจาก การนำข้อมูลของบุคคลไปใช้ในทางที่มิชอบ

2.3 กฎหมายอาชญากรรมทางคอมพิวเตอร์ (Computer Related Crime)

อันมีวัตถุประสงค์ในการคุ้มครองสังคม จากความผิดที่เกี่ยวกับข้อมูลข่าวสาร อันถือเป็นทรัพย์ที่ไม่มีรูปร่าง (Intangible Object)

แต่ทว่ามีค่ายิ่งในยุคแห่งเทคโนโลยีสารสนเทศ

2.4 กฎหมายการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Electronic Data Interchange: EDI)

ที่จะเอื้ออำนวยให้มีการ ทำนิติกรรมสัญญากันทางอิเล็กทรอนิกส์ได้

2.5 กฎหมายลายมือชื่อทางอิเล็กทรอนิกส์ (Electronic Signature Law)

ที่มีวัตถุประสงค์ในการสร้างความมั่นคงให้กับคู่กรณีในอันที่จะต้องพึ่งพาเทคโนโลยีเพื่อการลงลายมือชื่อ

2.6 กฎหมายการโอนเงินทางอิเล็กทรอนิกส์ (Electronic Funds Transfer)

มีวัตถุประสงค์ในการคุ้มครองผู้บริโภคและสร้างหลักประกันที่มั่นคง ในการทำธุรกรรมทางการเงินดังกล่าว

2.7 กฎหมายโทรคมนาคม (Telecommunication Law)

มุ่งวางกลไกในการเปิดเสรีให้มีการแข่งขันที่เป็นธรรม และจัดให้องค์กรกำกับดูแลที่เป็นกลาง และมีประสิทธิภาพรวมทั้งสร้างหลักประกันให้ประชาชนสามารถเข้าถึงบริการโทรคมนาคมได้อย่างทั่วถึง (Universal Service) ซึ่งหน่วยงานที่เกี่ยวข้องโดยตรง เช่น กระทรวงคมนาคม มีการดำเนินการอยู่แล้วกฎหมายระหว่างประเทศ องค์การระหว่างประเทศ และการค้าระหว่างประเทศที่เกี่ยวเนื่องกับเทคโนโลยีสารสนเทศ

2.8 กฎหมายที่เกี่ยวเนื่องกับอินเตอร์เน็ต

2.9 กฎหมายพัฒนาเทคโนโลยีและอุตสาหกรรมอิเล็กทรอนิกส์และคอมพิวเตอร์

2.10 กฎหมายทรัพย์สินทางปัญญา

ดำเนินมาตรการที่จะเร่งรัดให้มีการคุ้มครองทรัพย์สินทางปัญญาอย่างเป็นรูปธรรม ทั้งในระยะสั้น เช่น การกำกับดูแล ให้เกิด ความถูกต้องตามกฎหมายลิขสิทธิ์ และในระยะยาว เช่น การให้ การศึกษากับเยาวชนในคุณค่าของทรัพย์สิน ทางปัญญา เป็นต้น

3. ความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์

หลักการพื้นฐานความปลอดภัยแบบ The CIA triad

ความมั่นคงปลอดภัย (security) คือ สถานะที่มีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ

ความมั่นคงปลอดภัยของสารสนเทศ (Information Security) คือ การป้องกันสารสนเทศและองค์ประกอบอื่น ๆ ที่เกี่ยวข้อง

ซึ่งรวมถึงระบบฮาร์ดแวร์ที่ใช้ในการจัดเก็บและโอนสารสนเทศนั้นด้วย

ความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์ จึงหมายถึง ความตระหนักและการป้องกันสารสนเทศและองค์ประกอบอื่น ๆ ที่เกี่ยวข้องกับพาณิชย์อิเล็กทรอนิกส์ ซึ่งรวมถึง ข้อมูล ซอฟต์แวร์ ระบบฮาร์ดแวร์ที่ใช้ในการจัดเก็บและถ่ายโอนสารสนเทศนั้นด้วย ซึ่งจะต้องสอดคล้องกับแนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

กลุ่มอุตสาหกรรมความมั่นคงปลอดภัยของคอมพิวเตอร์ ได้กำหนดแนวคิดขึ้นเรียกว่า The CIA triad ดังนี้

ความมั่นคงปลอดภัยของสารสนเทศ นั้นมีองค์ประกอบด้วยกัน 3 ประการ คือ

-ความลับ (Confidentiality)

-ความถูกต้อง ความสมบูรณ์ (Integrity)

-ความพร้อมใช้ (Availability)

ทรัพย์สิน (Asset) ที่มีความมั่นคงปลอดภัยนั้นต้องประกอบด้วยองค์ประกอบทั้ง 3 อย่างครบถ้วน ไม่ว่าทรัพย์สินนั้นจะเป็นสิ่งที่จับต้องได้ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย หรือทรัพย์สิน ที่จับต้องไม่ได้ เช่น ข้อมูล เป็นต้น

1. Confidentiality (ความลับ)

   เป็นการรับประกันว่า ผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้

   สารสนเทศที่ถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิ์หรือไม่ได้รับอนุญาต จะถือเป็นสารสนเทศที่เป็นความลับถูกเปิดเผย ซึ่งองค์กรต้องมีมาตรการป้องกัน เช่น

   - การจัดประเภทของสารสนเทศ
   - การรักษาความปลอดภัยให้กับแหล่งข้อมูล
   - การกำหนดนโยบายความมั่นคงปลอดภัยและนำไปใช้งาน
   - การให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและนำไปใช้

2. Integrity (บูรณภาพ ความถูกต้อง ความสมบูรณ์)

บูรณภาพของข้อมูล คือ ความถูกต้องสมบูรณ์ ความครบถ้วน และไม่มีสิ่งปลอมปน ทั้งก่อน-ระหว่าง-และภายหลังการกระทำการใดๆ กับข้อมูลชุดนั้น ดังนั้น สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องและครบถ้วน เช่น ถูกทำให้เสียหาย ไฟล์หาย เนื่องจา virus, worm หรือ Hacker ทำการปลอมปน สร้างความเสียหายให้กับข้อมูลองค์การได้ ยอดเงินในบัญชีธนาคารหรือแก้ไขราคาในการสั่งซื้อ

3. Availability (สภาพพร้อมใช้)

สารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบอื่นที่ได้รับอนุญาตเท่านั้น หากเป็นผู้ใช้ระบบที่ไม่ได้รับอนุญาต การเข้าถึงก็จะล้มเหลวถูกขัดขวาง เช่น การป้องกันให้เครื่องและระบบให้บริการพาณิชย์อิเล็กทรอนิกส์มีสภาพพร้อมใช้งาน สามารถให้บริการได้เสมอ ป้องกัน รับมือ ตอบสนอง และบรรเทาความเสียหายเมื่อถูกโจมตีได้ ดังนั้น จึงต้องมีการระบุตัวตน (Identification) ว่าเป็นสมาชิกและพิสูจน์ได้ว่าได้รับอนุญาตจริง (Authorization)

The CIA triad Extension

เพิ่มเติมจาก CIA Triangle เพื่อให้ครอบคลุม ดังนี้

- Authenticity – การพิสูจน์ตัวจริง (Authentication) พร้อมกับการมอบสิทธิ์ (Authorization)
- Accountability – ความรับผิดชอบ เป็นการรับประกันว่าธุรกรรมต้องสามารถตรวจสอบหลักฐานภายหลังได้
- Non-repudiation – การไม่สามารถบอกปัดความรับผิด เป็นการรับประกันว่าธุรกรรมต่างๆ สามารถทวนสอบความถูกต้องได้

16. หน่วยสมรรถนะร่วม (ถ้ามี)

N/A

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

N/A

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

18.1 เครื่องมือการประเมิน

1. แบบทดสอบปรนัย ชนิด 4 ตัวเลือก
2. แบบประเมินการสัมภาษณ์
3. แบบประเมินแฟ้มสะสมงาน

หรือ

4. RESK

ดูรายละเอียดจากคู่มือการประเมิน

18.2 เครื่องมือการประเมิน

1. แบบทดสอบปรนัย ชนิด 4 ตัวเลือก
2. แบบประเมินการสัมภาษณ์
3. แบบประเมินแฟ้มสะสมงาน

หรือ

4. RESK

ดูรายละเอียดจากคู่มือการประเมิน

18.3 เครื่องมือการประเมิน

1. แบบทดสอบปรนัย ชนิด 4 ตัวเลือก
2. แบบประเมินการสัมภาษณ์
3. แบบประเมินแฟ้มสะสมงาน

หรือ

4. RESK

ดูรายละเอียดจากคู่มือการประเมิน

1. รหัสหน่วยสมรรถนะ 2021

2. ชื่อหน่วยสมรรถนะ บริหารจัดการระบบความมั่นคงปลอดภัยด้านเว็บไซต์

3. ทบทวนครั้งที่ 1 / 2566

4. สร้างใหม่ ☐ **ปรับปรุง** ☑

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

นักบริหารระบบความมั่นคงปลอดภัยด้านพาณิชย์อิเล็กทรอนิกส์

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

บุคคลที่ทำหน้าที่เกี่ยวกับการวางแผนเพื่อบริหารจัดการเว็บไซต์ได้อย่างมั่นคงปลอดภัย การตั้งค่าเครื่องบริการเว็บได้อย่างมั่นคงปลอดภัย การใช้โปรแกรมประยุกต์บนเครื่องบริการเว็บเพื่อให้บริการได้อย่างมั่นคงปลอดภัย การรับมือสถานการณ์ภัยคุกคามที่เกิดกับเว็บไซต์ได้อย่างมีประสิทธิภาพ

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☐	☑	☐	☐

8. กลุ่มอาชีพ (Sector)

กลุ่มวิชาชีพอุตสาหกรรมดิจิทัล สาขาธุรกิจดิจิทัลและพาณิชย์อิเล็กทรอนิกส์

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

N/A

10. ข้อกำหนดหรือกฎระเบียบที่เกี่ยวข้อง (Licensing or Regulation Related) (ถ้ามี)

N/A

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
20211 วางแผนเพื่อบริหารจัดการความมั่นคงปลอดภัยเว็บไซต์	1. วางแผนงานด้านความมั่นคงปลอดภัยของเว็บไซต์ 2. คัดเลือกผู้รับจดทะเบียนชื่อโดเมน 3. คัดเลือกเครื่องบริการเว็บ 4. คัดเลือกระบบบริหารจัดการเว็บไซต์ (CMS)	ข้อสอบข้อเขียน การสัมภาษณ์ แฟ้มสะสมผลงาน
20212 ตั้งค่าความมั่นคงปลอดภัยเครื่องบริการเว็บได้	1. กำหนดค่าคอนฟิกโปรแกรมสำหรับให้บริการเว็บ (Web server software) 2. กำหนดค่าคอนฟิกระบบบริหารจัดการเว็บไซต์ (CMS) 3. กำหนดค่าคอนฟิกระบบฐานข้อมูล (Database system) 4. กำหนดค่าคอนฟิก Server-side Script Engine 5. กำหนดและรักษารหัสผ่าน	ข้อสอบข้อเขียน การสัมภาษณ์ แฟ้มสะสมผลงาน

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
20213 ใช้โปรแกรมประยุกต์ความมั่นคงปลอดภัยบนเครื่องบริการเว็บเพื่อให้บริการ	1. เลือกใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค SQL Injection 2. เลือกใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค OS Command Injection 3. เลือกใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค Unchecked Path Parameter 4. เลือกใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค Improper Session Management 5. เลือกใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค Cross-site Scripting 6. เลือกใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค Cross-site Script Request Forgery (CSRF) 7. เลือกใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค HTTP Header Injection 8. เลือกใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค Mail Header Injection 9. เลือกใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากการไม่มีระบบพิสูจน์ตัวจริงและการกำหนดสิทธิ์ (Lack of Authentication and authorization)	ข้อสอบข้อเขียน การสัมภาษณ์ แฟ้มสะสมผลงาน
20214 รับมือสถานการณ์ภัยคุกคามที่เกิดกับเว็บไซต์	1. เตรียมการรับมือภัยคุกคามที่เกิดขึ้นกับเว็บไซต์ 2. เลือกใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ 3. จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ 4. สำรองข้อมูลและกู้คืนเว็บไซต์ได้	ข้อสอบข้อเขียน การสัมภาษณ์ แฟ้มสะสมผลงาน

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

N/A

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. ปฏิบัติการวางแผนเพื่อบริหารจัดการเว็บไซต์ได้อย่างมั่นคงปลอดภัย
2. ปฏิบัติการตั้งค่าเครื่องบริการเว็บได้อย่างมั่นคงปลอดภัย
3. ปฏิบัติการใช้โปรแกรมประยุกต์บนเครื่องบริการเว็บเพื่อให้บริการได้อย่างมั่นคงปลอดภัย
4. ปฏิบัติการรับมือสถานการณ์ภัยคุกคามที่เกิดกับเว็บไซต์ได้อย่างมีประสิทธิภาพ

(ข) ความต้องการด้านความรู้

1. ภัยคุกคาม มัลแวร์ การโจมตีเว็บไซต์ชนิดต่างๆ
2. การวางแผนและบริหารเพื่อป้องกัน ตรวจหา และโต้ตอบต่อภัยคุกคาม มัลแวร์ การโจมตีเว็บไซต์ชนิดต่างๆ
3. การบริหารระบบการให้บริการอีคอมเมิร์ซและเว็บไซต์
4. กฎหมายที่เกี่ยวข้องกับการให้บริการอีคอมเมิร์ซและเว็บไซต์

14. หลักฐานที่ต้องการ (Evidence Guide)

หลักฐานที่ต้องการจะกำหนดข้อแนะนำเกี่ยวกับการประเมิน และควรที่จะใช้ประกอบร่วมกันกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. เอกสารรับรองการปฏิบัติงานหรือผลการประเมินการปฏิบัติงานจากสถานประกอบการ
2. เอกสารการประเมินจากการจำลองสถานการณ์โดยใช้กรณีศึกษา
3. เอกสารการประเมินการสัมภาษณ์
4. แฟ้มสะสมผลงาน

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. เอกสารผ่านการอบรมเกี่ยวกับการบริหารระบบอีคอมเมิร์ซและเว็บไซต์
2. เอกสาร วุฒิบัตร หรือใบรับรองที่แสดงว่าผ่านการทดสอบ (Certificate)
ด้านการบริหารความมั่นคงเกี่ยวกับระบบคอมพิวเตอร์ทั้งแบบอิงและไม่อิงผลิตภัณฑ์จากหน่วยงานที่เกี่ยวข้อง
3. เอกสารรับรองการผ่านการสอบข้อเขียนหรือผลการทดสอบความรู้

(ค) คำแนะนำในการประเมิน

ประเมินเกี่ยวกับการบริหารระบบความมั่นคงปลอดภัยอีคอมเมิร์ซและเว็บไซต์ โดยพิจารณาจากหลักฐานที่เกี่ยวข้องทั้งหลักฐานการปฏิบัติงานและหลักฐานด้านความรู้

(ง) วิธีการประเมิน

1. พิจารณาหลักฐานความรู้
2. พิจารณาหลักฐานการปฏิบัติงาน

15. ขอบเขต (Range Statement)

ขอบเขตอธิบายถึงขอบเขตของการปฏิบัติงาน และสภาพแวดล้อมอื่น ๆ หรือสถานการณ์อื่น ๆ ที่มีผลกระทบต่อการทำงาน รวมถึงเครื่องมือ อุปกรณ์ เทคโนโลยี ทรัพยากรที่ใช้ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

(ก) คำแนะนำ

การบริหารระบบความมั่นคงปลอดภัยอีคอมเมิร์ซและเว็บไซต์
ผู้เข้ารับการประเมินจะต้องแสดงการทดสอบเกี่ยวกับการวางแผนเพื่อบริหารจัดการเว็บไซต์ได้อย่างมั่นคงปลอดภัย การตั้งค่าเครื่องบริการเว็บได้อย่างมั่นคงปลอดภัย การใช้โปรแกรมประยุกต์บนเครื่องบริการเว็บเพื่อให้บริการได้อย่างมั่นคงปลอดภัย การรับมือสถานการณ์ภัยคุกคามที่เกิดกับเว็บไซต์ได้อย่างมีประสิทธิภาพ

(ข) คำอธิบายรายละเอียด

1. การวางแผนเพื่อบริหารจัดการเว็บไซต์ จะต้องจัดทำแผนด้านความมั่นคงปลอดภัยของเว็บไซต์ได้ตามมาตรฐานที่กำหนด
เลือกผู้รับจดทะเบียนชื่อโดเมนได้อย่างเหมาะสมกับวัตถุประสงค์การใช้งาน หาแนวทางการเลือกรูปแบบเครื่องบริการเว็บได้อย่างมีประสิทธิภาพ
และหาแนวทางการเลือกระบบบริหารจัดการเว็บไซต์ (CMS) ได้อย่างมีประสิทธิภาพ
2. การตั้งค่าเครื่องบริการเว็บ จะต้องตั้งค่าโปรแกรมสำหรับให้บริการเว็บ (Web server software) ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด
ตั้งค่าระบบบริหารจัดการเว็บไซต์ (CMS) ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด ตั้งค่าฐานข้อมูล (Database system) ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด ตั้งค่า Server-side Script Engine ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด และกำหนดและรักษารหัสผ่านได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด
3. การใช้โปรแกรมประยุกต์บนเครื่องบริการเว็บ จะต้องใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค SQL Injection ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด
ใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค OS Command Injection ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด

ใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค Unchecked Path Parameter ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด
ใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค Improper Session Management ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด
ใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค Cross-site Scripting ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด ใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค Cross-site Script Request Forgery (CSRF) ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด ใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค HTTP Header Injection ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด ใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากเทคนิค Mail Header Injection ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด และใช้โปรแกรมประยุกต์เพื่อป้องกันการโจมตีจากการไม่มีระบบพิสูจน์ตัวจริงและการกำหนดสิทธิ์ (Lack of Authentication and authorization) ได้เหมาะสมตามเกณฑ์มาตรฐานที่กำหนด

4. การรับมือสถานการณ์ภัยคุกคามที่เกิดกับเว็บไซต์ (Incident Handling) จะต้องรับมือภัยคุกคามที่เกิดขึ้นกับเว็บไซต์ได้อย่างมีประสิทธิภาพ ใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ได้อย่างมีประสิทธิภาพ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ และสำรองข้อมูลเว็บไซต์ได้อย่างมีประสิทธิภาพ

5. ตามมาตรฐานที่กำหนด ตามเกณฑ์มาตรฐานที่กำหนด และ ได้อย่างมีประสิทธิภาพ หมายถึง การปฏิบัติการที่สอดคล้องกับแนวปฏิบัติ ข้อกำหนด เกณฑ์ หรือมาตรฐานที่เกี่ยวข้องกับ เช่น ETDA Recommendation on ICT Standard for Electronic Transactions ขมธอ. 4 – 2559, NIST SP 800-44 Guidelines on Securing Public Web Servers, OWASP Open Web Application Security Project, ข้อกำหนดที่เกี่ยวข้องจากข้อแนะนำแก้ไขและป้องกันข้อบกพร่องหรือจุดอ่อนของเว็บไซต์ ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต (Thai CERT), คู่มือ “How to Secure Your Website” ของ สำนักงานส่งเสริมเทคโนโลยีสารสนเทศ ประเทศญี่ปุ่น (Information-Technology Promotion Agency (IPA), Japan) , ISO/IEC 27001 เป็นต้น

16. หน่วยสมรรถนะร่วม (ถ้ามี)

N/A

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

N/A

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

18.1 เครื่องมือการประเมิน

1. แบบทดสอบปรนัย ชนิด 4 ตัวเลือก
2. แบบประเมินการสัมภาษณ์
3. แบบประเมินแฟ้มสะสมงาน

หรือ

4. RESK

ดูรายละเอียดจากคู่มือการประเมิน

18.2 เครื่องมือการประเมิน

1. แบบทดสอบปรนัย ชนิด 4 ตัวเลือก
2. แบบประเมินการสัมภาษณ์
3. แบบประเมินแฟ้มสะสมงาน

หรือ

4. RESK

ดูรายละเอียดจากคู่มือการประเมิน

18.3 เครื่องมือการประเมิน

1. แบบทดสอบปรนัย ชนิด 4 ตัวเลือก
2. แบบประเมินการสัมภาษณ์
3. แบบประเมินแฟ้มสะสมงาน

หรือ

4. RESK

ดูรายละเอียดจากคู่มือการประเมิน

18.4 เครื่องมือการประเมิน

1. แบบทดสอบปรนัย ชนิด 4 ตัวเลือก
2. แบบประเมินการสัมภาษณ์
3. แบบประเมินแฟ้มสะสมงาน

หรือ

4. RESK

ดูรายละเอียดจากคู่มือการประเมิน